Probability of Data Leakage and its Impacts on Confidentiality

Paul Simon and Scott Graham
Air Force Institute of Technology, Wright-Patterson AFB, Ohio, USA
paul.simon.ctr@afit.edu
scott.graham@afit.edu

Abstract: A multi-channel communication architecture featuring distributed fragments of data is presented as a method for improving security available in a communication architecture. However, measuring security remains challenging. The Quality of Secure Service (QoSS) model defines a manner by which the probability of data leakage and the probability of data corruption may be used to estimate security properties for a given communication network. These two probabilities reflect two of the three aspects of the IT security triad, specifically confidentiality and integrity. The probability of data leakage is directly related to the probability of confidentiality and may be estimated based on the probabilities of data interception, decryption, and decoding. The number of listeners who have access to the communication channels influences these probabilities, and unique to the QoSS model, the ability to fragment and distribute data messages across multiple channels between sender and receiver. To simulate the behaviors of various communication architectures and the possibility of malicious interference, the probability of data leakage and its constituent metrics require a thorough analysis. Even if a listener is aware that multiple channels exist, each intermediate node (if any) simply appears to have one input and one output. There may be one or more listeners, and they may or may not be working cooperatively. Even if the listener(s) gains access to more than one channel, there is still the challenge of decrypting, decoding, or reassembling the fragmented data. The analysis presented herein will explore the probability of confidentiality from both the authorized user's and the adversary's perspective.

Keywords: confidentiality, communications modeling, probability, security, metrics, data leakage

1. Introduction

Accurate and repeatable metrics describing confidentiality and integrity of communications through contested environments would be useful. The Quality of Secure Service (QoSS) model, defined by Simon et al. (2021) and Simon et al. (2022), provides a quantitative method to describe security of communications available to authorized users. Security, in this context, refers to confidentiality, integrity, and availability of the path between transmitter and receiver. While availability metrics are common, confidentiality and integrity are difficult to quantify, therefore surrogate metrics of probability of data leakage and probability of data corruption are used. The QoSS model further considers existence of adversarial listeners and malicious disruptors. While it may be relatively easy to recognize when a disruptor is injecting malicious data, it is challenging to detect adversarial actors eavesdropping on communications. It is also difficult to know an adversary's capability or intention. Tools exist to limit what eavesdroppers are able to receive. However, the QoSS model adds the ability to quantify how much data the eavesdropper may be able to receive. Due to the difficulty in quantifying security, probabilistic models are useful in conjunction with simulations. Exercising simulations many times provides insight into unexpected emergent behaviors.

The primary contribution of this work is to explore the impact data fragmentation has on the probability of data leakage from both authorized user's perspective and adversarial listener's perspective. Since the probability of leakage is a surrogate for the probability of confidentiality, this simulation analysis provides insight into available communication system security, despite adversarial interaction. Section 2 of this paper presents an overview of the QoSS model. Section 3 relates simulation results of multiple communication architectures based on the QoSS model. Section 4 provides analysis on how those simulation results may be perceived by an authorized user or an adversary. Section 5 highlights future research and provides a conclusion.

2. Background

The QoSS model details a manner by which the probability of data leakage and the probability of data corruption may be calculated for a given communication network. These two probabilities reflect two of the three aspects of the IT security triad, specifically confidentiality and integrity. Other authors, such as Almerha et al. (2010), attempt to frame the IT security triad based on arbitrary routing metrics or, like Hughes et al. (2013), by developing security requirements for confidentiality and integrity. Leon et al. (2010) attempt to develop an all-encompassing organizational matrix to measure security, whereas Wang et al. (2008) use the Common Vulnerability Scoring System (CVSS) to quantify vulnerabilities as a surrogate. Unlike most traditional models, availability in the QoSS model reflects strictly physical capabilities of an architecture. This, in turn, leaves all

malicious interactions with the architecture, notably eavesdropping, jamming, or spoofing, considered under confidentiality and integrity.

According to the QoSS model, the probabilities of leakage and corruption are based on six characteristics of a communication architecture, possible interactions with malicious listeners and disruptors, and the number of communication channels available. The characteristics are probability of interception, probability of decryption, probability of decoding, probability of injection, probability of suppression, and probability of noise. The probability of leakage, specifically, is estimated based on the probabilities that a transmitted message may be intercepted, decrypted, and decoded. A receiver, authorized or not, is not guaranteed to successfully receive, decrypt, or decode messages. This approach is inspired by the analysis developed by Sweet et al. (2018).

Some communication systems allow for multiple parallel heterogeneous channels to exist between transmitter and receiver. One example is Signaling System 7 (SS7), detailed by Modarressi et al. (1990) and Russell (2002), used in analog telephone networks. Another example developed by Khisti et al. (2012) uses two independent parallel channels to limit the amount of information leakage if either are intercepted. Redundant Array of Inexpensive Disks (RAID) systems, detailed by Hennessy et al. (2002), allow the ability to fragment and distribute data across multiple disks for security purposes. Even TCP/IP networks allow for fragmentation of data into packets that comply with the Maximum Transmission Unit (MTU) of the network, although those strategies, highlighted by Creedon et al. (2009), are strictly to optimize the performance of a single TCP/IP connection. Modern networking also employs the use of intermediate nodes to provide flexible relaying and routing across broad networks. In a complex architecture that features multiple channels and multiple intermediate hops similar to the one shown in Figure 1, even if a listener is aware that multiple channels exist between endpoints **A** and **D**, each intermediate node (if any) simply appears to have one input and one output. There may be one or more listeners, and they may or may not be working cooperatively. Further, even if the listener(s) gains access to more than one channel, there is still the challenge of decrypting and decoding or reassembling the fragmented data. As such, the overall calculation for the probability of leakage, *P(l)*, is defined as

$$P(l) = \frac{P(int) \cdot P(dcr) \cdot P(dco) \cdot \sigma}{n}$$

where *P(int)* is the probability of interception, *P(dcr)* is the probability of decryption, *P(dco)* is the probability of decoding, σ is the number of adversarial listeners who are able to access the channel(s), and *n* is the number of channels between transmitter and receiver. These metrics comprise the probability of leakage, and

$$P(C) = 1 - P(l)$$

where *P(C)* is the probability of confidentiality. We assume that the maximum number of listeners, whether they are cooperating or not, cannot exceed the number of channels.

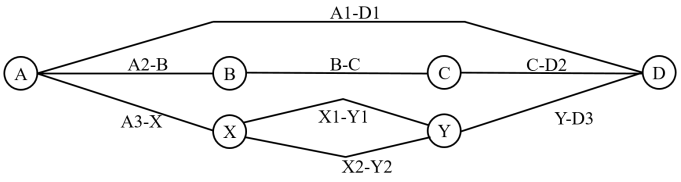

Figure 1: Hybrid communication network featuring three heterogeneous channels between **A** and **D**

This research focuses on security of communications as defined by the QoSS model. We are developing a representative simulation environment of communication architectures with varying complexity and featuring multiple heterogeneous channels and intermediary nodes. This architecture is in contrast to separately routing critical information over secure channels or maintaining multiple other levels of security, as proposed by Winjum et al. (2008), which is similar to the multi-level security model presented by Jin et al. (2012). Typically, communication systems are simulated using Markov chains because the mathematical models are tractable. However, due to the difficulty in defining security, understanding security within an architecture similar to the one shown in Figure 1 for both authorized and unauthorized users becomes intractable. The goal of the simulation environment is to quantify confidentiality with an eye toward developing more secure communication architectures through the creation of a comprehensive protocol that splits data across multiple

channels with varying amounts of cross-channel duplication, checksum, or CRC overhead. Messages must also be received correctly and discourages eavesdropping despite the possible malicious injections and recognizing which channel is being targeted. This simulation represents one of many possible approaches to implementing and quantifying the security available within a communication network.

By simulating various architectures ranging from single point-to-point connections to multi-channel, multi-hop architectures, and by varying the data transmitted across those channels, it becomes clear that the probability of leakage and its constituent metrics have a complex relationship to system confidentiality. The simulations provide anecdotal evidence that a multi-channel architecture may limit the useful information an eavesdropper receives. The probabilities of interception and decoding, and the amount of fragmentation and duplication across channels demonstrate useful emergent performance characteristics of confidentiality from both the authorized user's and the adversarial listener's perspective.

3. Analysis of simulation

Test cases in the simulation environment observe the security aspects of various communication architectures, ranging from a single point-to-point channel to a single channel with five intermediary relay nodes, to five parallel heterogeneous channels with five intermediary relay nodes. Additional nodes and channels do not appear to add insight. Each communication link, for example **A1-D1**, **C-D2**, or **A3-X** in Figure 1, is programmed to have specific probabilities of interception and decoding. To simplify the simulation process, probability of decryption is set to 1, implying that no encryption is used in these systems. For simplicity and brevity, test cases presented herein are limited to a two-channel and a three-channel system using ASCII-encoded data to observe the simple readability of the alphabet as transmitted through the system. These rudimentary tests reflect the data confidentiality.

3.1 Messages and fragments

The same 8-bit ASCII-coded message is used for all simulations. It is transmitted across the architecture, and, based on the probability of interception, an adversary intercepts the message or it does not. Based on the probability of decoding, the adversary does or does not decode the message. It is irrelevant if the adversary is able to decode a message if they do not receive it. It is possible to have duplicative or cooperative listeners. Multiple listeners may work cooperatively and share intercepted data, but that may affect the probability of decoding since properly merging the intercepted data may prove difficult. For this study, we assume one adversarial listener, but that listener may have access to one, several, or all of the channels within an architecture. The listener accesses the communications between relay nodes, for example **A2-B**, **B-C**, or **C-D2** from Figure 1, simulating on-the-wire or over-the-air connections. If the listener were located in nodes, that would allude to compromised hardware, which is a different challenge outside the scope of this research. If the listener is on any one link, then the entire channel is compromised because all information from that channel is available. In that case, we only consider the worst probability of interception across any given channel.

These aspects of the simulation point directly to harnessing the channels in different ways. One method is simply to duplicate data over multiple channels. This method is ideal for ensuring tamper-free messages during transmission.

Another method involves splitting messages across the multiple channels to prevent unauthorized access to the information. There are numerous methods of fragmenting and distributing messages across the available channels. Poly et al. (2016) developed a detailed analysis of multi-channel communications with respect to maintaining privacy. Castro-Medina et al. (2019) perform a review of fragmentation and duplication for cloud-based systems. Kapusta et al. (2015) describe fragmentation for distributed storage systems. Feng et al. (2015) describe self-adaptive fragmentation for large files to reduce overhead. Another approach uses the Trivium cypher with TLS to distribute data across channels, detailed by Hayden et al. (2020). For simplicity, the following examples use a round-robin technique of distributing data across channels. These techniques are intended to further increase security by shuffling what data appears on which channels.

For example, message *M* is eight 8-bit ASCII-encoded characters, for a total of 64 bits of data. For this example, there are n=2 channels and the duplication factor, DF=1, meaning that no data is duplicated on the two channels. Assuming that *M* is split into two, four, or eight equally sized fragments, k, then the total number of bits per fragment is 32, 16, or 8 bits, respectively. These fragments maintain the byte-wise alignment of the ASCII

characters. As there are two channels, each channel transmits one, two, or four fragments. With more fragments, there are more opportunities for rudimentary scrambling. A mechanism to reassemble the original message correctly is assumed contained in the receiver. Therefore, in the examples shown in Figure 2, if an eavesdropper has access to only one of the channels, then the eavesdropper only intercepts at most half of the original message, equal to the average loading (*AL*) of the channel.

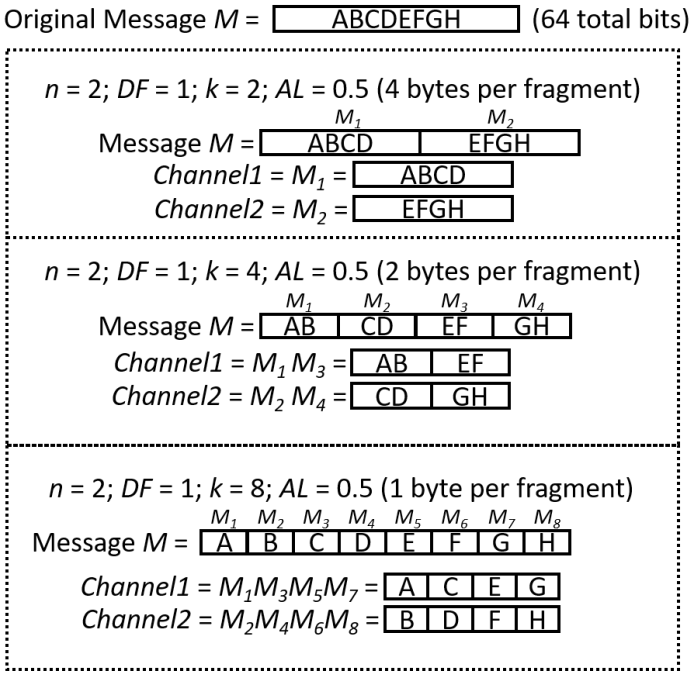

Figure 2: Byte-wise fragmentation of original message across two channels

Figures 3 and 4 show the 64-bit message *M* split into smaller fragments, such that each fragment is 4 bits or 1 bit, respectively. If the sixteen 4-bit fragments were distributed across two channels, an eavesdropper would again only have access to half of the total message, although the bits appear random if ASCII-encoding is assumed. It is interesting to note that in Figure 2, the lightly scrambled data on channel 1 appears to be a series of ASCII letter "D", while meaningful information is transmitted on channel 2.

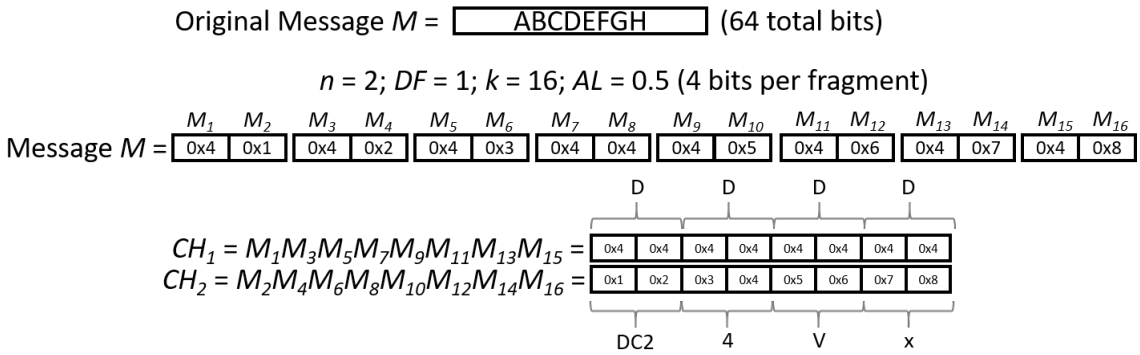

Figure 3: 4-Bit fragmentation of original message across two channels

If the 64 one-bit fragments shown in Figure 4 are distributed across two channels, the amount of data on each channel remains half of the original message. In this case, the reassembly protocol must interleave the two channels as they are received, increasing the complexity of the receiver. The scrambled bits on each channel do not appear to be in any pattern, especially if they are assumed to be ASCII-encoded text.

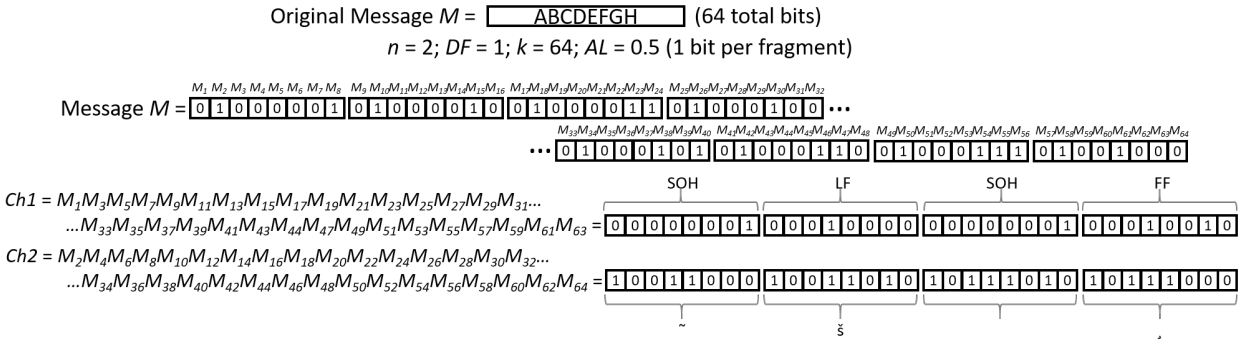

Figure 4: 1-Bit fragmentation of original message across two channels

Figures 5 through 7 show another example system utilizing three parallel channels. To avoid uneven division, message *M* is twelve 8-bit ASCII-encoded characters, for a total of 96 bits. For this example, there are *n*=3 channels and *DF*=1, meaning no data is duplicated. Figure 5 shows the examples with *M* split into two, four, or eight fragments, *k*, for a total number of 32, 16, or 8 bits per fragment, respectively. These fragments maintain the byte-wise alignment of the ASCII characters. Each of the channels transmits one, two, or four fragments. Because there are three channels, if an eavesdropper accesses one channel, they intercept at most one third of the original message, equal to the average loading (*AL*) of the channel. However, a key difference between this example and that of Figure 2 is if the eavesdropper captures two channels, they only receive two thirds of the original message, and there may be no clear manner of reassembly.

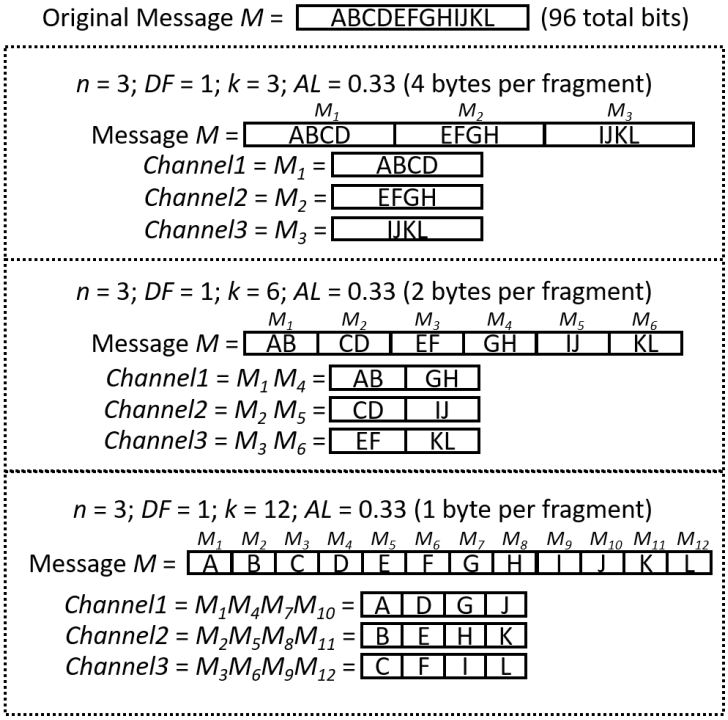

Figure 5: Byte-wise fragmentation of original message across three channels

The 96-bit message *M* is split into smaller fragments, as shown in Figures 6 and 7, such that each fragment is four bits or one bit, respectively. An eavesdropper would again have access to one third of the total message bits if a single channel were intercepted. An unexpected alignment in the ASCII-encoded text occurs between channels 2 and 3 of the 1-byte fragment example and channels 1 and 3 of the 4-bit fragment example. In both examples, channel 3 provides the same information, although context for correct reassembly does not exist. Additional research is needed to verify if this is a coincidental anomaly or indications of a broader pattern.

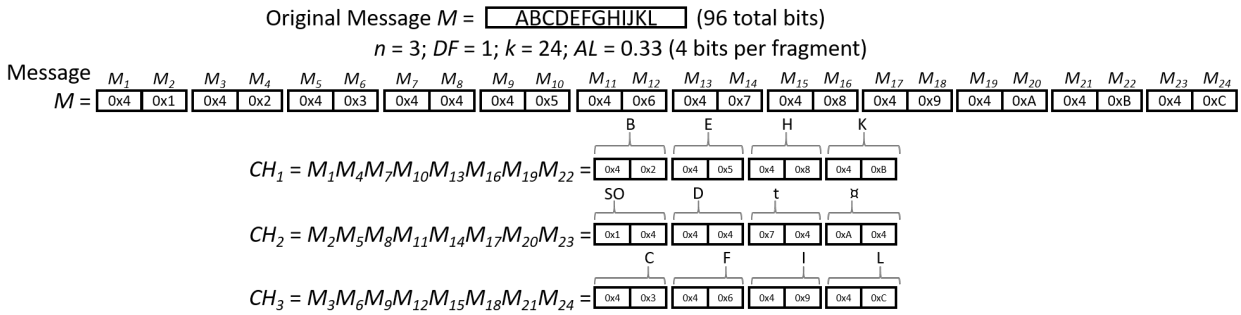

Figure 6: 4-Bit fragmentation of original message across three channels

If the 96 one-bit fragments shown in Figure 7 are distributed across three channels, the amount of data on each channel remains one third of the original message. The scrambled bits on each channel do not appear to be in any pattern, especially when compared to the examples shown in Figures 5 and 6. If an adversary intercepts two of three channels in this example, the information received jumps to two-thirds of the original message. As every third bit of the original message is missing, reconstructing and decoding the message remains difficult.

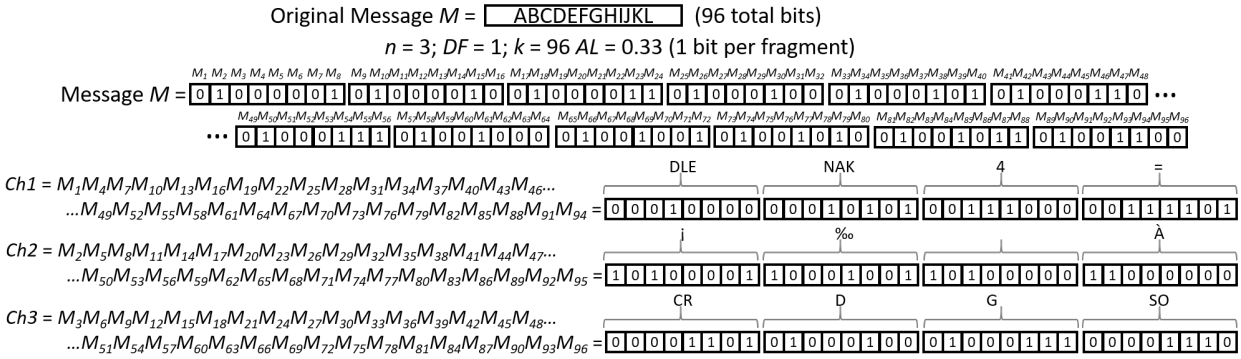

Figure 7: 1-Bit fragmentation of original message across three channels

3.2 Probability of interception and probability of decoding

To estimate data leakage, the probabilities of interception and decoding and amount of fragmentation are applied to the multiple channels. This is a surrogate estimation for the overall security available on a communication architecture.

As an example, we assume the probability of interception, *P(int)*=0.5, for all channels, the probability of decoding, *P(dco)*=0.5, and the probability of decryption, *P(dcr)*=1, which means there is no encryption on any of the channels. The calculation for *P(l)* becomes

$$P(l) = \frac{0.5 \cdot 1 \cdot 0.5 \cdot \sigma}{n} = \frac{0.25 \cdot \sigma}{n}$$

which indicates that *P(l)*=0.25 for any channel, yielding a probability of confidentiality, *P(C)*=0.75. If σ=0 listeners, there is no leakage. In the example network where *n*=2 channels, *P(l)* becomes

$$P(l) = \frac{0.5 \cdot 1 \cdot 0.5 \cdot \sigma}{2} = \frac{0.25 \cdot \sigma}{2} = 0.125 \cdot \sigma.$$

Therefore, the maximum *P(l)*=0.25. If σ=1 listener, *P(l)*=0.125. For every additional channel used, *P(l)* is further reduced. This assumes data is not duplicated across channels; duplicated data requires modifying the equations.

By comparison, in the example network where *n*=3 channels, *P(l)* becomes

$$P(l) = \frac{0.5 \cdot 1 \cdot 0.5 \cdot \sigma}{3} = \frac{0.25 \cdot \sigma}{3} = 0.083 \cdot \sigma.$$

Therefore, when σ=1 listener, $P(I)$=0.083; when σ=2 listeners, $P(I)$=0.166. The maximum $P(I)$=0.25.

The simulation environment confirms these results for messages transmitted across various network configurations. Based on network metrics, the observation is that leakage is approximately the percentage of bits of a message that an adversary successfully receives and decodes. Therefore, as suggested by simulation and despite the possible presence of adversarial listeners and the added complexity of the transmission/reception protocol, increasing the number of channels and maintaining a minimal amount of duplication across channels significantly reduces the probability of leakage, in turn increasing the probability of confidentiality.

4. Implications

The results may be viewed from two perspectives, that of the authorized user and that of the eavesdropper. The authorized user, in most cases, wants as little information to be intercepted by the eavesdropper as possible. The ideal case is exactly zero bits being intercepted, although a limited amount of intercepted data may be acceptable as long as it is not useful. Conversely, the eavesdropper wants to collect as much information as possible. The ideal case is to collect, decrypt, and decode all information. However, this suggests a specific minimum amount of data that must be intercepted to be useful. Because of these opposing viewpoints, the implications must be assessed from both the authorized user's perspective and from the adversarial perspective.

4.1 From the user's perspective

From the authorized user's perspective, to achieve secure communications and reduce possible data leakage, the simulation environment points to two possible solution sets. One solution is to use strong encryption for all transmissions. It is irrelevant if an eavesdropper is able to intercept messages if they are not able to decrypt them. However, many systems are unable to perform necessary encryption processes. In these cases, the second solution set may be useful.

The second solution utilizes multiple parallel channels and distributes message fragments across those channels with minimal duplication. The technical hurdles contained in this solution include: the transmitter must set up and maintain numerous separate channels; the receiver must accurately reconstruct the data; the system must maintain minimal latency; and the system must appear as a single point-to-point connection. Modern communication networks have mastered the ability to minimize latency, whereas this architecture would harness that requirement across multiple connections, while also managing possible timing disparities, jitter, or potentially lost packets or channels. Pitkanen et al. (2008) addresses some of these challenges.

The probability of leakage presents a trade space between security and network complexity. As demonstrated in the simulation environment, with data split evenly (DF=1 and AL=0.5 across two channels), an adversary with access to only one channel has access to 50% of the data. Across three channels with the same amount of fragmentation, the adversary's challenges become harder. Furthermore, due to the size of the fragments and the manner those fragments are assembled into the transmission packets, the probability of decoding the data also decreases. Since the original message is split evenly across two or three channels, the overall time the connection must be maintained is reduced, thus possibly reducing the temporal opportunity for exploitation. These benefits continue to increase with four or more channels.

Clearly, the more channels that are instantiated, the more complex the system becomes. If each channel is routed differently, there is no guarantee that data packets from each channel will be received at the same time. This obviates the need for a reassembly protocol that enumerates the received packets and recombines the fragments correctly. These are technical trade-offs that exist within most technologies. However, in situations where using encryption is not an option, at least there is some opportunity to thwart eavesdroppers through the use of rudimentary scrambling and multiple channels.

A third solution set does exist and may be applied to situations where driving data leakage to zero is imperative. In those cases, to ensure near-absolute security, the original message may be encrypted and then fragments of the encrypted message may be distributed across multiple channels, similar to the techniques that Ciriani et al. (2010) propose. Each fragment may also be encrypted before transmission for added confidentiality. This would have the ultimate effect of layering protection mechanisms, possibly to a degree beyond the capabilities of the

eavesdropper and driving the probability of leakage to near zero. This solution adds additional technical challenges to achieve exceptionally high levels of security.

4.2 From the adversary's perspective

Estimating capabilities and intentions of an adversarial listener is always challenging. Hu et al. (2019) develop a model to analyze the possibility, goals, and capabilities of an eavesdropper. Without any additional information about the adversary, a logical assumption is that an adversary has equal or greater knowledge or capabilities than an authorized user. In this research, a foundational assumption is that the adversary is aware of other channels, and of the potential to fragment data across multiple channels. A second assumption is that they are aware of the protocols used in the transmitter and receiver. However, the number of utilized channels, the channel characteristics, and the size and distribution of the data fragments remain unknown to the adversary.

The challenge for the eavesdropper is to align the probabilities of interception, decryption, and decoding. If strong encryption is used, then the data the eavesdropper intercepts, regardless of number of channels or fragments, will appear to be randomized data. However, in the cases where encryption is not used, the adversary has a reasonable opportunity to intercept data, and systems that do not utilize encryption will be targeted.

Ignoring the challenges of receiving specific coherent transmissions on different physical media, exploiting a communication system begins with intercepting a message transmission. If the architecture utilizes a single wired or wireless channel between transmitter and receiver, the adversary must tap into the physical media without revealing themselves. If, for example, data is transmitted across a single channel that has multiple intermediate relay nodes, any of those connections will provide the same data, thus the whole channel is compromised. If the architecture utilizes two channels and splits the data equally between the two channels, the eavesdropper with access to one of the two channels has access to at most 50% of the data. If the two channels have multiple intermediary nodes, those provide additional points for infiltration. If the eavesdropper gains access to both channels simultaneously, then the eavesdropper has access to 100% of the data. As more channels are introduced, it becomes more challenging to intercept all those channels simultaneously, especially if they feature path diversity. The eavesdropper may be able to discern the existence of additional channels based on the message and packet formation, but that does not guarantee successfully finding and intercepting them.

The probability of decoding is the other key factor in the adversary's calculations, specifically reassembling and decoding the intercepted message. Much like an eavesdropper listening into a conversation, they need to figure out the content and context of the communications. They cannot assume that data is ASCII-based text, or even English language based. The data may appear scrambled, but additional information may be available about the messages elsewhere. Based on partial reassembly of the message or based on educated guess, the adversary may determine the existence of other channels, or they may determine what portions of the message are missing. Depending on the value of the target, the eavesdropper may take additional measures to discover techniques used in transmitting the messages. It must be assumed that the eavesdropper is relentless and, with a sufficient portion of data intercepted, will eventually discover any secret.

5. Conclusion

These simulation results point to improved data security. Fragmenting data across multiple communication channels demonstrates potential improvements to confidentiality through a method of scrambling across a distributed attack surface. The challenge of reconstructing data from multiple channels may push an adversary to reach a point of diminished returns. Future research will focus on incorporating data fragmentation across multiple channels into a protocol suite that will reside between the application layer and the TCP/IP stack. These initial simulation results will guide future protocol development to further improve communication security with various feedback mechanisms or encryption. In the end, no security mechanism is completely secure, but better mechanisms require more time and effort to defeat. Understanding what security is available in a communication network will allow designers to focus on developing techniques and technologies to keep adversaries one step behind or with a small fragment of their ultimate goal: useful information.

Acknowledgements

Funded in part by the Air Force Institute of Technology, Center for Cyberspace Research. The views expressed in this paper are those of the authors, and do not reflect the official policy or position of the United States Air

Force, Department of Defense, or the U.S. Government. This document has been approved for public release, case number 88ABW-2022-0037

References

Almerhag, I. A.; Almarimi, A. A.; Goweder, A. M. and Elbekai, A. A. (2010). Network security for QoS routing metrics. *International Conference on Computer and Communication Engineering, ICCCE'10*, (May), 11–13. https://doi.org/10.1109/ICCCE.2010.5556868

Castro-Medina, F.; Rodríguez-Mazahua, L.; Abud-Figueroa, M. A.; Romero-Torres, C.; Reyes-Hernández; L. Á., and Alor-Hernández, G. (2019). Application of data fragmentation and replication methods in the cloud: a review. In *2019 international conference on electronics, communications and computers (CONIELECOMP)* (pp. 47-54). IEEE.

Ciriani, V.; Vimercati, S.D.C.D.; Foresti, S.; Jajodia, S.; Paraboschi, S. and Samarati, P. (2010) Combining fragmentation and encryption to protect privacy in data storage. ACM Transactions on Information System Security (TISSEC), Vol. 13, 1–33.

Creedon, E. and Manzke, M. (2009). Impact of fragmentation strategy on ethernet performance. In 2009 Sixth IFIP International Conference on Network and Parallel Computing (pp. 30-37). IEEE.

Feng, L.; Zhang, Y. and Li, H. (2015) Large file transmission using self-adaptive data fragmentation in opportunistic networks. In Proceedings of the 2015 Fifth International Conference on Communication Systems and Network Technologies, Gwalior, India, 4–6 April.

Hayden, M.; Graham, S.; Betances, A. and Mills, R. (2020) Multi-Channel Security through Data Fragmentation. In Proceedings of the IFIP International Conference on Critical Infrastructure Protection, Arlington, VA, USA, 16 March; pp. 137–155.

Hennessy, L.J. and Patterson, D.A. (2011) Co.mputer Architecture: A Quantitative Approach; Elsevier: Amsterdam, The Netherlands.

Hu, Z., Vasiliu, Y., Smirnov, O., Sydorenko, V., & Polishchuk, Y. (2019). Abstract Model of Eavesdropper and Overview on Attacks in Quantum Cryptography Systems. In *2019 10th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS)* (Vol. 1, pp. 399-405). IEEE.

Hughes, J. and Cybenko, G. (2013) Quantitative metrics and risk assessment: The three tenets model of cybersecurity. Technology Innovation Management Review. Vol. 2, 3, 15–24.

Jin, J. and Shen, M. (2012). Analysis of Security Models Based on Multilevel Security Policy. *Management of E-Commerce and E-Government (ICMeCG), 2012 International Conference on*, 95–97. https://doi.org/10.1109/ICMeCG.2012.72

Kapusta, K. and Memmi, G. (2015). Data protection by means of fragmentation in distributed storage systems. In *2015 International Conference on Protocol Engineering (ICPE) and International Conference on New Technologies of Distributed Systems (NTDS)* (pp. 1-8). IEEE.

Khisti, A. and Liu, T. (2014). Private broadcasting over independent parallel channels. *IEEE Transactions on Information Theory*, *60*(9), 5173–5187. https://doi.org/10.1109/TIT.2014.2332336

Leon, P.G. and Saxena, A. (2010) An approach to quantitatively measure information security. In Proceedings of the 3rd India Software Engineering Conference, Mysore, India, 25–27 February.

Modarressi, A.R. and Ronald, A.S. (1990) Signaling system no. 7: A tutorial. IEEE Communication Magazine, Vol. 28, 19–20.

Pitkanen, M.; Keranen, A. and Ott, J. (2008) Message fragmentation in opportunistic DTNs. In Proceedings of the 2008 International Symposium on a World of Wireless, Mobile and Multimedia Networks, Newport Beach, CA, USA, 23–26 June. (pp. 1-7). IEEE.

Pohly, D.J. and Patrick, M. (2016) Modeling Privacy and Tradeoffs in Multichannel Secret Sharing Protocols. In Proceedings of the 2016 46th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), Toulouse, France, 28 June–1 July.

Russell, T. (2002) Signaling System # 7; McGraw-Hill: New York, NY, USA; Vol. 2.

Simon, P.M.; Graham, S.; Talbot, C. and Hayden, M. (2021) Model for Quantifying the Quality of Secure Service. Journal of Cybersecurity and Privacy, Vol. 1, 289–301.

Simon, P.M. and Graham, S. (2022) Extending the Quality of Secure Service Model to Multi-Hop Networks. . Journal of Cybersecurity and Privacy, Vol. 1-4, 793-803.

Sweet, I.; Trilla, J.M.C.; Scherrer, C.; Hicks, M. and Magill, S. (2018) What's the Over/Under? Probabilistic Bounds on Information Leakage. In International Conference on Principles of Security and Trust; Springer: Cham, Switzerland.

Wang, J.A.; Xia, M. and Zhang, F. (2008) Metrics for information security vulnerabilities. Journal of Applied Global Research. Vol. 1, 48–58.

Winjum, E. and Berg, T. J. (2008). Multilevel security for IP routing. *Proceedings - IEEE Military Communications Conference MILCOM*, 1–8. https://doi.org/10.1109/MILCOM.2008.4753318.